REMARKS

Claims 1-22 are pending. All pending claims are in condition for allowance.

Alleged Applicant Admitted Prior Art (AAPA)

In the Office Action dated October 2, 2009, the Office rejected independent claims 1 and 10-13 under alleged Applicant Admitted Prior Art (AAPA), citing to page 3, lines12-17; page 6, lines 23-29; page 21, lines 13-27; page 22, line 23 - page 23, line 2; page 25, lines 5-14; page 25, line 23 - page 26, line 2; and page 27, lines 4-12.

Applicants consider the subject matter of each alleged AAPA.

page 6, lines 23-29: This passage states, in its entirety: "Furthermore, if the required passcode is short, i.e. less than 7 digits or letters, the time-consuming task of entering a long passcode is reduced and the possibility of entering an erroneous passcode is reduced. High security may still be achieved by utilising high-security PIN methods such as the one described in C. Gehrmann and K. Nyberg, "Enhancements to the Bluetooth baseband security", Proceedings of the NordSec Conference 2001, Nov. 1-2, 2001, DTU Denmark." Applicants do not claim any method of processing PINs to achieve high security from a short PIN. Indeed, nothing in the claims relates to processing PINs at all. Accordingly, this allegedly AAPA is inapposite to the claims. Note the passage at page 27, lines 4-12 cites the identical paper.

page 21, lines 13-27: Although the Office cited the entire paragraph, the only subject matter that could be considered an admission of prior art is lines 23-27: "An example of such an algorithm [for generating pseudo random numbers] is a pseudo random function based on a one way hash function such as the HMAC algorithm described in H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message authentication", IETF RFC 2104 (obtainable on

http://www.ietf.org/rfc/rfc2104)." Applicants do not claim any pseudo random number algorithm. Accordingly, this allegedly AAPA is inapposite to the claims.

page 22, line 23 - page 23, line 2: The only relevant portion of this citation is p. 22, line 28 – p. 23, line 1, which states, "The MAC algorithm used to calculate the MAC may be any suitable MAC algorithm, preferably a cryptographically strong MAC algorithm. An example of such a MAC algorithm providing a high level of security is the HMAC algorithm (see e.g. H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message authentication", IETF RFC 2104, obtainable on http://www.ietf.org/rfc/rfc2104)." While, e.g., claim 2 recites calculating and including a MAC as integrity protection, no MAC algorithm is claimed. Accordingly, this allegedly AAPA is inapposite to the claims. Note the passage at page 25, line 23 - page 26, line 2 cites the identical paper.

The two remaining citations to alleged AAPA both refer to Bluetooth shared link key encryption during Bluetooth pairing. The passage at page 3, lines12-17 states:

> The Bluetooth pairing mechanism produces a shared secret, the so-called link key, between two Bluetooth devices (see "Baseband Specification" in "Specification of the Bluetooth System, Core, Version 1.1", Bluetooth Special Interest Group, February 2001). The link key is derived from a PIN that is entered by the user of the devices. The link key is subsequently used to protect the Bluetooth communication.

This passage describes one mode of the pairing mechanism of the Bluetooth protocol. A link key is derived from a PIN, and the link key is used to encrypt communications between paired devices.

Note the very sentence following this passage, on page 3, lines 17-21: "However, since the remote access to a subscription module is particularly security sensitive, there is a need for increased security, i.e., an **improved** protection of the subscription module against unauthorised access to the sensitive subscription information and services on the module." In

the same paragraph in which they describe the known Bluetooth pairing mechanism, Applicants note that it provides insufficient security for "particularly security sensitive" accesses such as to a subscription module, and that **improved** protection – that is, improved protection over what the Bluetooth pairing offers – is necessary.

Applicants further explain this point with reference to Figure 1, depicting a client device 106 accessing a subscription module 102 on a server device 101 over a Bluetooth link 115 between the two devices. In particular, at page 18, lines 14-22, Applicants state:

> As mentioned above, the security offered for the communications link 115 by standard wireless communications protocols, such as Bluetooth, do not provide sufficient security for the security sensitive subscription module access. According to the invention, the processing units 105 and 107 provide functionality 103 and 109, respectively, for integrity protection of the messages sent over the communications link 115. Hence, it is ensured that the messages have not be [sic.] altered during transmission over the air interface 115, and that the messages were sent from an authorised device.

(emphasis added). Accordingly, the integrity protection is explicitly and repeatedly described as being in addition to the simple, known link key encryption provided by the Bluetooth pairing protocol.

During patent examination, the pending claims must be given their broadest reasonable interpretation consistent with the specification. MPEP § 2111. "The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction 'in light of the specification as it would be interpreted by one of ordinary skill in the art.'" *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). In *In re Prater*, 415 F.2d 1393, 1404-05 (CCPA 1969), the predecessor to the Federal Circuit explained that "reading a claim in light of the specification, to thereby interpret limitations explicitly recited in the claim, is a quite different thing from 'reading limitations of the specification into a claim,' to thereby narrow the scope of the claim."

Any claim rejection that equates a simple link key encryption, such as the Bluetooth shared link key pairing, to the claimed integrity protection, is necessarily an interpretation of integrity protection that is not the "broadest reasonable interpretation consistent with the specification." MPEP § 2111. The specification clearly states that link key encryption is insufficient, and more secure communication requires integrity protection. Whatever integrity protection means, it manifestly means greater security than Bluetooth link key encryption, and hence cannot be the same thing.

The citation to page 25, lines 5-14 merely describes the client device 106 and server device 101 forming a conventional Bluetooth communication link, using a shared Bluetooth link key, as described above (page 3, lines12-17). For the same reasons described above, this passage cannot reasonably be equated to the claimed integrity protection, which Applicants' specification repeatedly states is required to overcome the lax security of shared Bluetooth link key encryption.

Claim 1

In the rejection of claim 1, the Office equates the claimed integrity protection to "using 'keys'" without further explanation or argument. This rejection is so broad, and so lacking of any specificity or identification of the prior art relied on, as to be virtually impossible to reply to. "[T]he particular part [of a prior art reference] relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified." 37 CFR § 1.104(c)(2). "The goal of examination is to clearly articulate any rejection early in the prosecution process so that the applicant has the opportunity to provide evidence of patentability and otherwise reply completely at the earliest opportunity." MPEP § 706. Applicants assume "using 'keys'" refers to the Bluetooth link key, as cited as AAPA.

Integrity protection is defined at page 5, lines 12-14: "Here, the term integrity protection comprises any method of assuring that information sent from an originating source is not accidentally or maliciously altered or destroyed during communication from the source to the receiver." As described (see page 3, lines 17-21; page 18, lines 14-22, both quoted above), conventional Bluetooth shared link key encryption based on a PIN provides insufficient security to ensure that a message is not "maliciously altered." As know by those skilled in the art, the same link key is used to encrypt every communication between Bluetooth paired devices over the duration of a pairing. In this environment, if the link key is intercepted, broken, or otherwise obtained, a message could be intercepted, decrypted, altered, re-encrypted, and re-transmitted to the destination. Integrity protection prevents this, by including information such as a message authentication code with each message, which is unique to that particular message. Accordingly, even if the Bluetooth link key is intercepted and the message decrypted, the destination device will know if the underlying message has been altered (for example, it will fail a hash test).

No alleged AAPA discloses, teaches, or suggests providing integrity protection of messages as recited in claim 1, when the claim terms are given their "broadest reasonable interpretation consistent with the specification." MPEP § 2111. For at least this reason, the rejection of claim 1 – whether under § 102 or § 103 – is improper and must be withdrawn.

The Office's citation, in the rejection of claim 1, to pages 4-5 of the specification is baffling. Those pages describe preferred embodiments of the invention. Nothing on pp. 4-5 describe any prior art or anything invented "by another."

Also, there is no reference to 802.11 in that passage. The only reference to 802.11 is on page 3, at lines 23-27: "Furthermore, the IEEE 802.11 standard offers secure communications services such as authentication and encryption via a wired equivalence privacy mechanism (see "IEEE Std 802.11 - 1999 Edition IEEE - Part 11: Wireless LAN Medium Access Control and

physical layer specifications"). However, this mechanism is known to have security weaknesses." Integrity protection goes beyond authentication and encryption. Nothing in the 802.11 protocol includes a unique message authentication code – or any other integrity protection information – in each message transmitted.

All dependent claims include all limitations of their respective parent claim(s), and thus also define patentable nonobviousness over the art of record.

Claim 8

Claim 8 recites the further step of determining whether a message from a client to the server device is authorized to address the subscription module. In rejecting the claim, the Office cited to p. 3, lines 12-17 and p. 7, lines 1-6 as alleged AAPA. The first citation describes the Bluetooth link key that is the basis for encryption of Bluetooth communications. "The link key is derived from a PIN that is entered by the user of the devices." This passage says absolutely nothing about determining whether any message is authorized to address any unit, much less whether a message from a client device to the server device is authorized to access a subscription module. Encrypted Bluetooth communications may comprise any information – such as voice telephone conversations between a cellphone and a headset. The mere existence of an encryption mechanism in Bluetooth provides no disclosure whatsoever regarding a determination of whether a client device is authorized to access a subscription module on a server device.

The second cited passage states, in its entirety:

> Hence, existing pairing mechanisms for the set-up of the communications link between the server and client devices may be utilised to enhance the security of the remote access to the subscription module. For example, in connection with a Bluetooth communication, the Bluetooth link key may be utilised to derive the shared secret for integrity protection. Hence, no additional interaction is required for achieving the additional security.

This states only that existing Bluetooth mechanisms – in particular, the link key – may be utilized to derive additional security mechanisms such as the inventive integrity protection. Nothing in this passage remotely suggests any determination whether a message from a client device to a server device is authorized to address a subscription module.

For at least the reason that the alleged AAPA fails to disclose the claimed limitations, the § 102 rejection of claim 8 is improper and must be withdrawn.

Claim 9

Claim 9 recites providing a shared secret between the client and server devices and access control list in the server device. The Office cited to p. 27, lines 4-7 as alleged AAPA; that passage simply states that a shared secret may be derived in a number of ways. This in no way discloses, teaches, or suggests the provision of a shared secret and an access control list related to the secret and the client device.

The Office then equated the claimed access control list to "cryptographic settings used between the client and the server." This claim interpretation is untenable. "[T]he words of the claim must be given their plain meaning unless the plain meaning is inconsistent with the specification." *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989). "Ordinary, simple English words whose meaning is clear and unquestionable, absent any indication that their use in a particular context changes their meaning, are construed to mean exactly what they say." *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1372 (Fed. Cir. 2004). "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*).

The plain meaning of "access control list," to one of skill in the art, is a list that controls access. A list is "a series of names, words, or other items written, printed, or imagined

one after the other." The American Heritage® Dictionary of the English Language, 4th ed., Houghton Mifflin Company, 2004. http://www.answers.com/topic/list, accessed January 04, 2010. Access is "the ability or right to approach, enter, exit, communicate with, or make use of." *Id.* Control is the "authority or ability to manage or direct." *Id.* Hence, an access control list is, first, a list. In particular, in the context of claim 9, those of skill in the art would consider it a list that functions to control access – e.g., a list of authorized users, a list of services or facilities a user is authorized to access, or the like. The access control list is explained in Applicant's specification at p. 26, lines 12-20, "In one embodiment, the information comprises an identifier identifying the client communications device, the shared secret K_m, and an access control list including the services of the subscription module which the communications device should be granted access to."

In stark contrast, cryptographic settings, as used in the rejection of claim 9, control only the mechanizations of encryption of communications. Cryptographic settings are, first, not a list. Second, they do not control access to anything – they merely define how messages are encrypted and decrypted. Nothing about how a message is encrypted during transmission has any impact on whether the device sending the message is authorized to access any particular service or function on the device receiving the message.

For at least the reason that the alleged AAPA fails to disclose the claimed limitations, and for the additional reason that the Office's interpretation of claim 9 goes far beyond the plain meaning of the claim terms, and would be regarded by those of skill in the art as manifestly unreasonable, the § 102 rejection of claim 9 is improper and must be withdrawn.

Claim 10-12, 13

The Office rejected claims 10-12 as "recit[ing] substantially the same limitations as recited in claim 1." For at least the reasons described above with respect to the rejection of claim 1, the Office has failed to establish that the alleged AAPA of Applicant's specification discloses each and every claimed limitation, arranged as in the claims. Accordingly, the rejection of claim 10 is improper and must be withdrawn. The Office rejected claim 13 as "recit[ing] substantially the same limitations as recited in claims 1 and 8 in combination." For at least the reasons described above with respect to the rejection of claims 1 and 8, the Office has failed to establish that the alleged AAPA of Applicant's specification discloses each and every claimed limitation, arranged as in the claims. Accordingly, the rejection of claim 13 is improper and must be withdrawn.

35 U.S.C. § 103 Rejections

In rejecting dependent claims 5, 7, 19, and 21 under § 103 over alleged AAPA in combination with other references, the Office has failed to establish a prima facie case of obviousness. As discussed above, the alleged AAPA of Applicant's specification fails to disclose the claimed limitations for which it is cited.

Conclusion

All dependent claims include all limitations of their respective parent claim(s), and thus also define patentable novelty and nonobviousness over the art of record. All pending claims are now in condition for allowance, which prompt action is hereby respectfully requested.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: January 13, 2010

Edward H. Green, III
Registration No.: 42,604

1400 Crescent Green, Suite 300
Cary, NC 27518

Telephone: (919) 854-1844
Facsimile: (919) 854-2084